

06/21/00
jc853 U.S. PTO

06-22-00

A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Brian A. LaMacchia
Docket: 154745.1/40062.65US03
Title: EVALUATING INITIALLY UNTRUSTED EVIDENCE IN AN EVIDENCE-BASED SECURITY POLICY

jc857 U.S. PTO
09/598814
06/21/00

CERTIFICATE UNDER 37 CFR 1.10

'Express Mail' mailing label number: EL387614538US

Date of Deposit: June 21, 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 and is addressed to BOX PATENT APPLICATION, Assistant Commissioner for Patents, Washington, D.C. 20231.

By: *Rita M. McAloon*
Name: Rita M. McAloon

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

We are transmitting herewith the attached:

- ☒ Transmittal sheet, in duplicate, containing Certificate under 37 CFR 1.10.
- ☒ Utility Patent Application: Spec. 41 pgs; 21 claims; Abstract 1 pgs.
The fee has been calculated as shown below in the 'Claims as Filed' table.
- ☒ 8 sheets of formal drawings
- ☒ Unsigned Combined Declaration and Power of Attorney
- ☒ A check in the amount of \$942.00 to cover the Filing Fee
- ☒ Return postcard

CLAIMS AS FILED

Number of Claims Filed		In Excess of:		Number Extra		Rate		Fee
Basic Filing Fee								\$690.00
Total Claims								
21	-	20	=	1	x	18.00	=	\$18.00
Independent Claims								
6	-	3	=	3	x	78.00	=	\$234.00
MULTIPLE DEPENDENT CLAIM FEE								\$0.00
TOTAL FILING FEE								\$942.00

Please charge any additional fees or credit overpayment to Deposit Account No. 13-2725. A duplicate of this sheet is enclosed.

MERCHANT & GOULD P.C.
P.O. Box 2903, Minneapolis, MN 55402-0903
(303) 357-1637

By: *Richard J. Holzer, Jr.*
Name: Richard J. Holzer, Jr.
Reg. No.: 42,668
Initials: RJH

**EVALUATING INITIALLY UNTRUSTED EVIDENCE
IN AN EVIDENCE-BASED SECURITY POLICY MANAGER**

Cross-reference to Related Applications

The present application is related to U.S. Patent Application No. _____, entitled EVIDENCE-BASED SECURITY POLICY MANAGER, and U.S. Patent Application No. _____, entitled FILTERING A PERMISSION SET USING PERMISSION REQUESTS ASSOCIATED WITH A CODE ASSEMBLY, filed concurrently herewith and assigned to the Assignee of the present invention.

Technical Field

The invention relates generally to computer security, and more particularly to evaluating evidence as input to an evidence-based security policy manager.

Background of the Invention

Security risks, such as allowing unauthorized access to a user's system, are inherent with many on-line activities. Therefore, security mechanisms have been developed to protect users' systems. For example, a user may download an on-demand application from the Internet and execute the application from within the browser. To prevent an unauthorized access to the user's system resources (e.g., a directory on the user's hard disk), the user's system is protected by "sandbox" security that is enforced within the browser environment. Sandbox security involves a limited, secure area of computer memory in which an application may execute, so that the application is prevented from accessing system resources that reside outside of the secure area.

In some circumstances, however, a user may wish to allow a downloaded application controlled access to certain resources within the user's system. For example, a user may wish to use an on-demand word processing application to generate a document and then save the document to a directory in the user's system.

Existing approaches for providing such applications with secure, controlled access to a user's system are too cumbersome and inflexible. In one method, for example, a security policy is defined within a policy database in which a given application is associated with a set of permissions. The security policy, in combination with origin information, signature information, and access restrictions, helps define a "trusted" relationship between the application and the user's system.

Consider the following example:

```
grant codeBase "http://www.BobsWidgets.com" signed by BobsCertificate {  
    permission lang.io.FilePermission "/tmp/" "read";  
    permission lang.io.FilePermission "/tmp/bwdir/*" "write";  
}
```

In the example, an applet from the source location, "www.BobsWidgets.com", is granted certain file access permissions if it is signed with a key corresponding to another key contained within BobsCertificate. An applet is traditionally a program designed to be executed from within a browser, rather than directly from within the operating system. The applet is granted permission to read files from the "/tmp" directory on the host system and to create and write to files in the "/tmp/bwdir" directory. Permission to "execute" is another common permission modifier. Other security policy specifications may, for example, grant broad permissions to access any file in any system location, regardless of the application's source or whether the

application is unsigned or signed.

In such approaches, a security policy manager uses self-verifying information, such as the certificate, to determine which permissions the applet (or any code assembly) should be granted.

However, in some situations, the information associated with the applet is not self-verifying and

5 may be considered “untrusted”. For example, assume that a user has installed an encryption

library on a computer system after purchasing a restricted license allowing the user to call the

library from a given application. At some later point, the user may attempt to download and

execute a different application that also includes calls to the encryption library. A code assembly

within the second application may include an embedded certificate, signed by the library vendor,

10 indicating that the code assembly vendor has also purchased rights to call the vendor’s library on

a user’s system. However, because the certificate is provided by the application vendor and not

the library vendor, the certificate may be untrusted.

By relying upon untrusted information, a policy manager may improperly grant

permissions to the applet or application and expose the system to security risks. The unanswered

15 problem is how to safely determine the appropriate permissions to be granted to a code assembly

using potentially untrustworthy information.

Summary of the Invention

In accordance with the present invention, the above and other problems are solved by associating a permission set with a code assembly based on evidence characterized by different

20 levels of trust (e.g., initially untrusted evidence and implicitly trusted evidence). Multiple

conditions are evaluated by a policy manager in association with individual elements of

evidence. Evidence can be received by the policy manager from a remote resource location,

from a local resource location (i.e., from within the computer system or from a storage peripheral coupled to the computer system), or from a membership criterion. The level of trust associated with a first element of evidence is independent of other evidence and conditions. The level of trust associated with a second element of evidence is dependent on a condition evaluated relative to the first element of evidence. If the multiple conditions are satisfied relative to the corresponding evidence, then the permission set is associated with the code assembly. The permission set is used in generating permission grant set used to control operation of the code assembly during run time.

In an implementation of the present invention, a method of associating a permission set with a code assembly based on evidence characterized by different levels of trust is provided. At least a first condition and a first element of evidence are received. The first condition is associated with the permission set and the level of trust associated with the first element of evidence is independent of other evidence and conditions. At least a second condition and a second element of evidence are also received. The second condition is associated with the permission set and the level of trust associated with the second element is dependent upon the first condition. The first condition is evaluated to determine whether it is satisfied by the first element of evidence. The second condition is evaluated to determine whether it is satisfied by the second element of evidence. The permission set is associated with the code assembly, if both the first condition and the second condition are satisfied.

In another implementation of the present invention, a policy manager for associating a permission set with a code assembly based on evidence characterized by different levels of trust is provided. A code collection generator generates a collection of code groups. Each code group is associated with a membership criterion and a permission set. A membership evaluator

evaluates at least a first condition and a second condition associated with one of the code groups to determine whether the code assembly is a member of the code group. The first condition applies a first element of evidence in the first condition. The level of trust associated with the first element of evidence is independent of other evidence and conditions. The second condition applies the second element of evidence. The level of trust associated with the second element is dependent upon the first condition. A permission set generator associates the permission set of the code group with the code assembly, if the code assembly is determined to be a member of the code group.

In other implementations of the present invention, articles of manufacture are provided as computer program products. One embodiment of a computer program product provides a computer program storage medium readable by a computer system and encoding a computer program for executing a computer process for associating a permission set with a code assembly based on evidence characterized by different levels of trust. Another embodiment of a computer program product may be provided in computer data signal embodied in a carrier wave by a computing system and encoding the computer program for associating a permission set with a code assembly based on evidence characterized by different levels of trust. The computer program product encodes a computer program for executing on a computer system a computer process for associating a permission set with a code assembly based on evidence characterized by different levels of trust. At least a first condition and a first element of evidence are received.

The first condition is associated with the permission set and the level of trust associated with the first element of evidence is independent of other evidence and conditions. At least a second condition and a second element of evidence is also received. The second condition is associated with the permission set and the level of trust associated with the second element is dependent

upon the first condition. The first condition is evaluated to determine whether it is satisfied by the first element of evidence. The second condition is evaluated to determine whether it is satisfied by the second element of evidence. The permission set is associated with the code assembly, if both the first condition and the second condition are satisfied.

5 These and various other features as well as other advantages, which characterize the present invention, will be apparent from a reading of the following detailed description and a review of the associated drawings.

Brief Description of the Drawings

FIG. 1 depicts an evidence-based security policy manager in an embodiment of the
10 present invention.

FIG. 2 represents a run-time call stack in an embodiment of the present invention.

FIG. 3 depicts a computer system for managing evidence-based security in an
embodiment of the present invention.

FIG. 4 depicts a policy manager for managing evidence-based security in an embodiment
15 of the present invention.

FIG. 5 depicts exemplary policy-levels on which a policy manager operates in an
embodiment of the present invention.

FIG. 6 illustrates a policy manager evaluating initially untrusted evidence in an
embodiment of the present invention.

20 FIG. 7 illustrates an exemplary system useful for implementing an embodiment of the present invention.

FIG. 8 illustrates a flow diagram of operations for associating a permission set with a code assembly based on evidence characterized by different levels of trust in an embodiment of the present invention.

Detailed Description of the Invention

5 An embodiment of the present invention provides an evidence-based policy manager that associates a permission set with a code assembly based on evidence characterized by different levels of trust (e.g., implicitly trusted evidence and initially untrusted evidence). "Initially untrusted" evidence may include evidence that is not trusted at the time it is received, although it may eventually be assigned a level of trust, depending on one or more conditions. Generally, a code assembly is a unit of packaged code, such as a .EXE file or a .DLL file. The policy manager can execute in a computer system (e.g., a Web client or a networked workstation) in combination with the verification module and class loader of the run-time environment; however, a policy manager can also execute outside of a run-time environment. The permission grant set generated for a code assembly is applied in the run-time call stack to help the system determine whether a given system operation by the code assembly is authorized. The policy manager may process permission requests received in association with the code assembly. Furthermore, both code assemblies and evidence may be received via a distribution mechanism, including a local source (e.g., from within the local machine), a local network or peripheral, or a remote resource location via a network (e.g., a communications connections such as the Internet).

20 The evidence may be characterized by different levels of trust. Conditions are applied to each piece of evidence. Each condition determines whether a given element of evidence is implicitly trusted or untrusted. If the condition treats the evidence as valid, independent of any

other evidence or condition, then the evidence is deemed implicitly trusted. Furthermore, chains of conditions may be configured to support recursive dependence relationships among sets of evidence, such as certificate path validation. In one embodiment of the present invention, the conditions are included in a membership criterion associated with a code group and a
5 corresponding permission set. The membership criterion is used to determine whether a given code assembly is a member of the code group, and therefore, qualified to be granted the permission set.

The policy manager may comprise execution modules for parsing a security policy, generating one or more code group collections, evaluating membership of the received code
10 assembly in one or more code groups, and generating a permission grant set. The policy manager may generate multiple policy-levels in accordance with a security policy definition specified in a security policy specification. Multiple policy levels may consist of multiple security policy descriptions that apply in combination to a particular code assembly for purposes of determining what permissions can be granted to the code assembly. For example, one policy
15 level may apply to all code that runs on the machine, and another might vary depending on the user currently logged in to the machine with respect to a particular execution of an assembly. Permission sets from each policy level may be merged to generate a permission grant set associated with the code assembly and applied in the run-time call stack of the execution thread.

FIG. 1 depicts an evidence-based security policy manager 104 in an embodiment of the
20 present invention. A resource location 100, such as a Web server, is accessible by a computer system 102 (e.g., a Web client or server) across a network (not shown). A resource location is commonly indicated by a URI (Uniform Resource Identifier), which is a generic term for all types of names and addresses that refer to objects on the World Wide Web. A URL (Uniform

Resource Locator) is a kind of URI. Exemplary resources may include without limitation documents, images, audio data, applications, routines, and other data and code datastores accessible through a network. It should be understood that a resource location may be local to the computer system 102 or remote to the computer system 102 (e.g., coupled by the Internet).

5 One type of resource relevant to an embodiment of the present invention is a code assembly. A code assembly may, for example, consist of applet code, application code, class code, routine code, and data. Code and data included in a code assembly may be in the form of byte-codes, intermediate code, machine code, or other code types, and data components (classes, images, audio and video clips, etc.). Furthermore, a code assembly may be packaged in an
10 archive file containing one or more classes downloaded from a resource location. In one embodiment of the present invention, classes of an application are combined into a module (an output of a linking process), and one or more modules may be combined into a code assembly.

FIG. 1 is described relative to a downloaded application executing on a computer system 102. Alternative embodiments may include downloaded applets, ACTIVEX controls,
15 and other routines and objects. An exemplary downloaded application consists of objects defined in one or more local or remote code assemblies. Local code assemblies are stored within the computer system 102 and are loaded into memory when needed. Remote code assemblies are downloaded from a resource location, such as resource location 100.

The computer system 102 initiates a run-time environment to execute the downloaded
20 application and to manage security of the computer system 102. The run-time environment on the computer system 102 may be initialized by a "trusted host", such as an operating system shell, a browser, an SQL server, or other code that is external to the run-time environment. The host, the loader 113, or some other shared resource initiates execution of the application by

downloading the various code assemblies 106 that constitute the application to the computer system 102 and passing the code assemblies 106 to a virtual machine 110 for execution.

A virtual machine provides a self-contained operating environment that performs much of the functionality of a separate computer. For example, an application can run in a virtual machine without direct access to the host operating system. This design has at least two advantages:

- System Independence: An application will run the same in any virtual machine that supports the programming language in which the application is written, regardless of the hardware and software underlying the system. For example, the same application (i.e., the same programming code) can run in a virtual machine on different computer systems having different types of microprocessors and different types of operating systems.
- Security: Applications running in a virtual machine are generally prevented from accessing protected system resources (i.e., the operating system, the file system, protected regions of memory, a connected network or peripheral). It should be understood, however, that an embodiment of the present invention can evaluate evidence and a security policy to determine whether to permit an application to access protected system resources. If permission for a given operation is granted, the application is considered “trusted” for that operation.

As the application components (e.g., downloaded code assemblies 106) are received by the computer system 102, a verification module 112 ensures that downloaded code in the code assemblies 106 is properly formatted and does not violate the safety restrictions of the code language or the virtual machine 110. Specifically, the safety restrictions that are to be enforced

prevent potentially malicious code from accessing data other than through the well-defined interfaces of the code. It is important that verified code be unable to examine or modify the granted permission sets that are associated with the code assembly through mechanisms that are inaccessible to the code assembly (i.e., accessible only to the execution environment). Other verifications, such as verifying that pointer addressing is not present, that internal stacks cannot overflow or underflow, and that code instructions will have the correct typed parameters, may also be performed. The code assemblies are then passed to a class loader 113, which can ensure that the application does not replace system-level components within the run-time environment (e.g., the class loader can force host-provided code assemblies to be executed when requested, thereby superceding name conflicts with downloaded code assemblies). Thereafter, the class loader 113 loads the code assemblies 106 onto a run-time call stack 114 in response to requests from the virtual machine 110.

For example, the virtual machine executes a first code assembly (e.g., main code assembly 202 of FIG. 2) that calls a routine provided by a second code assembly (e.g., parser code assembly of FIG. 2). The class loader 113 receives the virtual machine's request for the second code assembly and loads the second code assembly into the run-time call stack 114 so that the first code assembly can call the needed routine.

In order to ensure that unauthorized accesses to protected areas are prevented, evidence 108 associated with each of the downloaded code assemblies 106 is input to the policy manager 104. Although evidence 108 is shown as being received from resource location 100, evidence 108 may also be received from one or more other resource locations or from within the computer system 102. For example, in one embodiment, an element of evidence may be hard-coded in the security policy specification 116, a configuration file, or a system registry.

Furthermore, evidence may be dynamically generated, internally or externally to the computer's system, responsive to receipt of the code assembly. The policy manager 104 determines the permission grant set associated with each code assembly. A security policy specification 116 is also input to the policy manager 104 to assist in the computation of appropriate grants. Based on these inputs, the policy manager 104 computes the appropriate grants for each code assembly and passes a resulting permission grant set to the run-time call stack 114.

As such, each code assembly in the run-time call stack 114 is associated with a corresponding permission grant set (e.g., permission grant sets 208, 210, and 212 in FIG. 2). A grant set is received from the policy manager and defines various permissions that have been computed for a corresponding code assembly. The permissions associated with each code assembly may vary widely based on the relative origin of the code assembly (e.g., local or remote), the specific origin of the code assembly (e.g., a specific URL), or other trust characteristics of the code assembly, all of which may be referred to as "evidence" 108. Exemplary trust characteristics may include cryptographic strong names, AUTHENTICODE signatures, and other security related evidence. In an embodiment of the present invention, evidence is used to determine a permission grant set for a given code assembly, method, module, or class. Furthermore, a security policy specification 116 may define multiple policy levels within a security framework for a given enterprise, machine, user, application, etc. in which the evidence of a given code assembly is evaluated.

FIG. 2 represents a run-time call stack 200 containing individual code assemblies that are stacked in the order in which they were called. The individual code assemblies may be downloaded from a remote resource location or may be retrieved locally from the computer system 102 of FIG. 1. The individual code assemblies are loaded into the run-time call stack 114

by the class loader 113 for access and execution by the virtual machine 110 in FIG. 1.

Alternatively, the grant sets 208, 210, and 212 may be stored separately from the stack 200 and accessed individually when required.

An alternative run-time call stack includes a slot for every method in a call chain. A grant set can be associated with each code assembly, class, module, or method in the call chain. In one embodiment, methods from a single assembly are associated with the same permission grant set. As such, the permission grant set need only be checked when the call chain transitions to a method in another code assembly (i.e., calls made within the same code assembly may not require a permission grant set check). Alternatively, methods, modules, or classes may be associated with distinct permission grant sets within the scope of the present invention.

For example, an object of the main application class in code assembly 202 is loaded first by the class loader into the illustrated run-time call stack 200. As the virtual machine executes the main class, the main class creates a parser object from a code assembly 204 and calls a method in the parser object to parse a data file in a protected area of the computer system. Accordingly, the class loader loads the parser code of the code assembly 204 into the run-time call stack 200. Thereafter, the parser object creates a file access object from a code assembly 206 and calls a method in the file access object to perform a read operation on the protected file. Accordingly, the class loader loads the file access code of the code assembly 206 into the run-time call stack 200.

Each permission grant set corresponds to a code assembly, method, module, or class in the run-time call stack. As such, a code assembly's attempt to access a protected resource is evaluated against its associated permission grant set, as well as the permission grant sets of other code assemblies in the run-time call stack 200. In the example of the read operation to the

protected file by the application illustrated in FIG. 2, the main code assembly 202 is associated with a permission grant set 208. The main code assembly 202 calls (as represented by arrow 214) a method in the parser code assembly 204, which is associated with the permission grant set 210. In order to access the protected file, the parser code assembly 204 calls (as represented by arrow 216) a method in the file access code assembly 206, which is associated with the permission grant set 212. In order to determine whether the file access code assembly 206 can access the protected file, the “intersection” of the permission grant sets 208 and 210 is calculated and used to determine whether the file access operation is permitted. For example, if the permission grant set 210 includes a permission to read from the protected file, but the permission grant set 208 does not, then access to the protected file is denied. In alternative embodiments, other logical operations may be employed to determine whether the file access operation is permitted.

Generally, an “intersection” operation (represented by the symbol “ \cap ”) is a set operation that yields the common elements of the operand sets. For example, if Set1 includes elements A, B, and C, and Set2 includes elements B, C, and D, then the intersection of Set1 and Set2 (i.e., Set1 \cap Set2) equals B and C. In contrast, a “union” operation (represented by the symbol “ \cup ”) is a set operation that yields all elements in the operand sets (i.e., the non-duplicative aggregation of all the elements in the sets). For example, if Set1 includes elements A, B, and C, and Set2 includes elements B, C, and D, then the union of Set1 and Set2 (i.e., Set1 \cup Set2) equals A, B, C and D.

FIG. 3 depicts a computer system for managing evidence-based security in an embodiment of the present invention. A server 300 is coupled to a client 302 via a

communications network (not shown). The client 302 executes a run-time environment (e.g., the COM+ 2.0 Run-time environment from Microsoft Corporation) to manage execution of applications on the client 302. In an embodiment of the present invention, the run-time environment includes a verification module 304, a loader module 306, and a policy manager 308.

5 As previously discussed, code assemblies are loaded into a run-time call stack 318 for execution by a virtual machine 312. A first category of code assembly is represented by local code assemblies 314, which are generally considered trusted code assemblies because they originate on the client 302. In contrast, a second category of code assembly is represented by downloaded code assemblies 316, which may originate from a remote or untrusted resource location, such as the server 300. Although local code assemblies 314 are generally trusted and downloaded code assemblies 316 are generally untrusted (at least initially), this convention may be controlled by the security policy specification 326 and may be modified to meet an administrator's needs. In an embodiment of the present invention, local code assemblies 314 and downloaded code assemblies 316 are input to the verification module 304 for verification. Thereafter, the code assemblies are input to the loader module 306 to be loaded into the run-time call stack 318.

The code assemblies 316 and 318 are generally associated with evidence (or credentials) used to compute a permission grant set for each code assembly. One exemplary evidence component may be an AUTHENTICODE signature. Another exemplary evidence component is a PICS (Platform for Internet Content Selection) label, which states properties of an Internet resource (e.g., executable code that has been virus checked). More details regarding a PICS label are discussed in P. Resnick and J. Miller, "PICS: Internet Access Controls without Censorship," Communications of the ACM, 39 (1996), pp. 87-93; also available at

www.w3.org/pub/WWW/PICS/iacwcv2.htm. Other examples of evidence may include, without limitation, proofs of purchase or license, author identifiers, vendor identifiers, versioning information, and programmatic credentials. Programmatic credentials, for example, may be in the form of program code that examines statements made by other credentials and fetches
5 supplementary information from the network before deciding which evidentiary statements to provide to the policy manager 308.

Evidence about a code assembly, method, module, or class may be provided by the host or extracted from the code assembly itself. Generally, local or host-provided evidence 322 is implicitly trusted and believed to be true, although this convention may be modified by the security policy. However, downloaded or assembly provided evidence 320 is generally untrusted
10 and must either be self-verifying (e.g., digitally-signed) or independently verified, although this convention may also be modified by the security policy. Downloaded evidence 320 may be downloaded from one or more resource locations and is not limited to evidence downloaded from the resource location from which the code assembly originates.

Local evidence 322 and downloaded evidence 320 are input to the security manager 308,
15 which evaluate the evidence based on the security policy. Within the policy manager 308, the evidence is evaluated in combination with the security policy specification 326 (and optionally permission requests 324, which define a permission set requested by the code assembly) to generate a final permission grant set that corresponds with a given code assembly.

20 Furthermore, because the verification process at the verification module 304 and the security management process at the policy manager 308 can execute concurrently, the two processes can communicate to affect each other. For example, the policy manager 308 may evaluate evidence indicating that a given code assembly is guaranteed to be type safe.

Accordingly, this type safety guarantee can be communicated to the verification module 304, which may skip a type checking operation based on the information. Alternatively, the verification module 304 may determine that a given code assembly does not pass a type safety check. In response, the verification module 304 may communicate with the policy manager 308 to query whether the code assembly has been granted a permission to execute despite the failure to pass a type safety check.

FIG. 4 depicts a policy manager for managing evidence-based security in an embodiment of the present invention. Executable components described relative to FIG. 4 may be implemented as software modules that are executable on a computer system. Alternatively, executable components implemented in hardware or in a combination of hardware and software are also contemplated in the scope of the present invention.

A policy manager 400 is coupled to receive a security policy specification 402 and an evidence set 404. The security policy specification 402 specifies a definition of one or more code groups, which may be used to define a category of related code assemblies (e.g., code assemblies signed by a given publisher). In one embodiment, the code groups are configured into one or more code group collections that may share some common characteristics. Alternatively, code groups may be configured into one or more code group hierarchies. An exemplary code group hierarchy 608 is illustrated in FIG. 6. The security policy specification may also define one or more policy levels. The evidence set 404 defines trust characteristics associated with a code assembly received by a computer system. Although the evidence set 404 is shown as originating outside of the policy manager 400, it should be understood that the policy manager may dynamically generate evidence that is evaluated by the membership evaluator 410.

Alternatively, evidence may be hard coded into a membership criterion associated with a code group generated by the code group generator 408.

10 In an embodiment of the present invention, a parser 406 receives the security policy specification 402 and extracts a definition of one or more code groups. Each code group is
5 associated with a membership criterion, a child definition (specifying zero or more child code groups of the code group), and a code-group permission set. The membership criterion specifies the conditions of membership for a given code group, which an evidence set must satisfy in order for a corresponding code assembly to be deemed a member of the code group. The child code group definition specifies the children of a given code group, although a child code group definition is not required in all code group collections. For example, in a non-hierarchical code collections, child definitions are likely to be omitted. If a code assembly proves membership in a first code group (i.e., a parent code group), the code assembly will be considered for membership in the child code groups of the parent code group. Code-group permission sets represent collections of permissions that may be assigned to code groups. If a code assembly is
15 determined to be a member of the code group, the permissions of the associated permission set may be granted to the code assembly, subject to other operations within the policy manager.

Other code group collection embodiments may include alternative data configurations. For example, in one embodiment, a code group collection is represented in a one-dimensional list of code groups, wherein each code group includes a membership criterion and a permission set,
20 and omits a child code group definition of the previous discussion. In this embodiment, the one-dimensional list may be ordered or unordered. Furthermore, other data configurations are contemplated within the scope of the present invention.

In an exemplary embodiment of the present invention, permission sets may be named to allow identification in the security policy specification 402. More than one code group may be assigned the same named permission set. As such, if a change is made to a named permission set (e.g., insertion or deletion of an individual permission), the change affects all of the code groups associated with that named permission set. For example, to grant the same permissions to several extranet business partner web sites that are members of different code groups, a single named permission set can be defined and assigned to the several code groups.

In an embodiment of the present invention, three types of named permission sets are supported: (1) standard permission sets –these sets are predefined and cannot be changed; (2) predefined permission sets – these sets may be modified by the administrator; and (3) custom permission sets – these sets may be defined by a user so long as the permission set names do not conflict with standard or predefined permission set names. In one embodiment, standard permission sets are available at all policy levels and may not be redefined in any individual policy level (universal scope). In this embodiment, the predefined and custom permission sets are defined and referenced within any given policy level and cannot be referenced from other policy levels (policy-level scope). It should be understood, however, that the scope of any permission set may extend beyond a given policy level in an alternative embodiment of the present invention.

Table 1 describes standard permission sets available in an embodiment of the present invention. Some standard permission sets, such as Internet and LocalIntranet sets, are predefined but may be modified by a user or an administrator. Other permission sets, such as SkipVerification, cannot be modified in an embodiment of the present invention. Alternative named permission sets are also contemplated within the scope of the present invention, and the

named permission sets described in Table 1 may be modified without departing from the present invention.

Standard Permission Sets	Description
Nothing	The associated code assembly has no permissions (i.e., to execute, to read, to write, to create, to append, to customize, to assert, to use, etc.).
Execution	The associated code assembly has permission to execute, but no other permissions to use protected resources.
Internet	The associated code assembly has the default permissions suitable for content from unknown origin, including permissions to execute, to open safe windows on the user interface to access the clipboard, to create its own application domain, to store a limited amount of data in a secure area, etc.
LocalIntranet	The associated code assembly has the default permissions suitable for content originating from within an enterprise, including permissions to access environment variables containing the user's current username and temporary directory locations, to execute and assert, to broadly access the user interface, to store a limited amount of data in a secure area, etc.
Everything	The associated code assembly has permissions from all standard name permission sets.
SkipVerification	The verification process or a portion thereof may be skipped, or the code assembly has permission to fail verification or a portion thereof.

Table 1 – Standard Permission Sets

The code-group permission set associated with a given code group may specify permissions associated with the code group. Alternatively, the code-group permission set associated with a given code group may specify permissions associated with the code group and all ancestor code groups. This flexibility allows a variety of security configurations (e.g., policy levels, permission sets, membership criteria, etc.) to be defined in a security policy specification. As discussed below, the policy manager may be developed to accommodate such a variety of security configurations.

In one embodiment, the security policy specification 402 may also specify multiple policy levels, each policy level having one or more code groups. The code groups may be configured into one or more code group collections or hierarchies. Policy levels allow an administrator, for example, to define different security policies for different machines, users, applications, time periods, user groups etc. When a membership evaluator 410 generates a policy-level permission set for a given policy level, the membership evaluator 410 traverses through the code groups associated with that policy level. The policy manager 400, therefore, can generate a permission set associated with the individual policy level. Thereafter, the permission sets from multiple policy levels may be processed (e.g., merged, selected, or filtered) to generate a resulting permission grant set 414.

Alternatively, the security policy specification 402 may specify one or more code group collections, and allocate the multiple policy levels across those code group collections. One method in which the allocation may be accomplished includes adding policy level properties to each code group. In this method, when the membership evaluator 410 traverses through the code group collections to determine the policy-level permission set for a given policy level, a code assembly is only determined to be a member of code groups associated with the policy level. To

process multiple policy levels in this embodiment, the one or more code groups (or code group hierarchies) are traversed once for each policy level. Alternative methods for managing code groups, code group collections, and policy levels are contemplated with the scope of the present invention.

5 In the illustrated embodiment, a code group collection generator 408 receives the parsed definition from the parser 406 and generates one or more code group collection in the memory of the computer system. The membership evaluator 410 receives the evidence set 404 and extracts trust characteristics relating to the corresponding code assembly. The membership evaluator 410 traverses through a code group collection (see FIG. 6 for an illustration of an exemplary code group hierarchy 608) to determine whether the code assembly is a member of one or more of the code groups within the code group collection. A permission set generator 412 receives the membership determination from the membership evaluator 410 and generates the appropriate permission grant set 414.

FIG. 5 depicts exemplary policy-levels on which a policy manager operates in an embodiment of the present invention. A security policy specification 500 is processed on the policy manager 502 to generate one or more security policy levels 506, 508, and 510 (this processing is represented by the dotted lines pointing to each of the policy levels). In an embodiment of the present invention, the security policy specification 500 is written as an XML (eXtensible Markup Language) expression. In alternative embodiments, however, other data
20 formats may be employed, including without limitation SGML (Standard Generalized Markup Language), HTML (HyperText Markup Language), RDF (Resource Description Framework), Visual Basic, and other standard and customized data and code formats.

0950834-062105
007299-4788756
10
5
In an embodiment of the present invention, the security policy specification 500 is a persistent representation of a security policy (e.g., an ordered collection of policy levels and/or code group collection), wherein each policy level is constructed of code groups. Lower order policy levels generally specify more restrictive policy restrictions than those of higher order policy levels. The security policy specification 500 is typically generated by a system administrator, a user, or an application setup program having appropriate permissions. Exemplary policy levels may include without limitation enterprise, machine, user, and application policy levels.

In one embodiment of the present invention, the highest level policy level is an enterprise policy level, which may define the security policy applied to all systems within any given enterprise. A lower policy level is a machine policy level, which may define the security policy applied to all users on a given system. A user policy level may define the security policy applied to a given user, regardless of which individual system the user is logged in to. An application policy level may define a security policy applied to a given application, regardless of the user or system executing the application. Additional policy levels and policy level orders are contemplated within the scope of the present invention.

20
The security policy specification 500 also manages security using one or more code group collections (e.g., hierarchical collections of code group levels), which are associated with membership criteria and contain or generate permission sets and special attributes. The security policy specification 500 consists of declarations of code groups with associated sets of permissions. A code assembly that is a member of a given code group may be granted permissions from the permission set associated with the code group. Code group membership is determined by the policy manager 502 using evidence set 504 associated with the code assembly,

such as a digital signature, the origin of the code assembly, etc. An administrator may add a code group to the code group collection in order to grant additional permissions to code assemblies belonging to the new code group.

In an embodiment of the present invention, a code group may be attributed with an “Exclusive” property flag, which specifies that only the permissions associated with this particular code group are to be applied to the member code assembly. Permission sets from other member code groups are ignored (i.e., not merged).

In an embodiment of the present inventions, code groups are defined in a code group hierarchy having a root node corresponding to “all” code assemblies. The root node represents a parent code group having child nodes, each of which may also have child nodes, and so on, to form a code group hierarchy. Alternative code group collections and hierarchies are also contemplated within the scope of the present invention including without limitation ordered and unordered lists of code groups. If the policy manager 502 determines a code assembly is a member of a parent code group, then the code assembly is tested against the children of the parent code group to determine membership therein. Exemplary code group types and membership criteria are described in Table 2, although other code group types are contemplated within the scope of the present invention. Furthermore, code group types may be associated with a property. For example, a code group type “software publisher” may be associated with a specified publisher, “Microsoft”, as in “Publisher: Microsoft”.

Code Group Types (label)	Membership Criterion Description
all code (“All Code”)	All code assemblies are deemed members of this code group.
software publisher (“Publisher”)	Code assemblies published by a specified publisher (e.g., Microsoft) and verified with a public key of a valid AUTHENTICODE signature are deemed members of this code group.
Zone (“Zone”)	Code assemblies originating from a specified zone of origin (e.g., Internet, LocalIntranet, RestrictedSites, etc.) are deemed members of this code group.
strong name (“Name”)	Code assemblies having a specified cryptographically signed name space (e.g., MS.Windows) are deemed members of this code group.
web site (“Site”)	Code assemblies originating from a specified web site (e.g., www.microsoft.com or *.microsoft.com, where “*” represents a wildcard character) are deemed members of this code group.
URL (“URL”)	Code assemblies originating from a specified resource location that includes a final wildcard character “*” (e.g., http://www.microsoft.com/app/*) are deemed members of this code group.

Table 2 – Exemplary Code Groups

Furthermore, the security policy specification 500 may define multiple policy levels. In the illustrated embodiment, each policy level (e.g., enterprise-level 506, machine-level 508, and user-level 510) has an individual code group hierarchy. As previously discussed, other policy

5 level configurations may be employed within the scope of the present invention, such as a configuration in which multiple policy levels are allocated across one or more code group

collections. For example, a single code-group hierarchy may have a single root node associated with multiple children, wherein each policy level is allocated to one child of the root node and the child's associated subtree.

In the illustrated embodiment, a policy-level permission set (e.g., enterprise-level permission set 512, machine-level permission set 514, or user-level permission set 516) is generated from each of the policy levels. A policy-level permission set merger 518 merges the policy-level permission sets 512, 514, and 516 to generate the permission grant set 520.

In an alternative embodiment, the policy-level permission set merger 518 may be replaced or supplemented by a policy-level permission set selector (not shown) to provide an alternative policy-level permission set generator. For example, in an embodiment of the present invention, a code-group permission set associated with an "exclusive" code group may supersede policy-level permission sets of other policy levels. As such, a policy-level permission set selector may be employed to select the code-group permission set associated with the "exclusive" code group, ignoring the policy-level permission sets of the other policy levels.

FIG. 6 illustrates a policy manager evaluating initially untrusted evidence in an embodiment of the present invention. Various pieces of evidence can be associated with different levels of trust. "Implicitly trusted" evidence refers to a suggestion of a given level of trust associated with the evidence (e.g., as applied within a membership criterion), whereas "initially untrusted" evidence refers to a suggestion of a given level of trust (or "distrust") upon receipt of the evidence by the policy manager. The level of trust assigned to a given piece of evidence need not be stated by the evidence itself nor need it be enforced uniformly within a given security policy or among multiple computer systems.

relative to one or more conditions associated with that evidence and that permission set.

However, the level of trust associated with “implicitly trusted” evidence is generally independent of any other evidence and conditions (e.g., conditions associated with other evidence). An exemplary element of implicitly trusted evidence is a host-stored key, which can be used to verify signed digital certificates received in association with a code assembly.

Another example of implicitly trusted evidence may be the URL from which the code assembly was downloaded, which is known by the host.

In contrast to implicitly trusted evidence, evidence received from other sources, such as the code assembly itself or from other resource locations, is generally deemed “initially untrusted”, although this convention may also be modified by the security policy. Generally, the level of trust eventually associated with “initially untrusted” evidence is dependent upon other evidence and conditions. If evidence is initially untrusted, independent validation of the initially untrusted evidence may allow the policy manager to rely on the evidence when granting the appropriate permission grant set to the code assembly. Independent verification, for example, can be performed using an element of implicitly trusted evidence. An exemplary element of initially untrusted evidence is a signed certificate of a third-party received in association with a code assembly, which can be verified by a host-stored key provided by the third-party (an exemplary element of implicitly trusted evidence).

A digital certificate establishes credentials for a code assembly and may be issued by a certification authority (CA). For example, a certificate may contain the code assembly vendor’s name, a serial number, expiration dates, a copy of the certificate holder’s public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the

certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509, for example.

A set of evidence 606 is received by the policy manager 600. Different elements of evidence may be received concurrently or at different times. Some elements of evidence may be received within a code assembly or merely referenced within a code assembly (e.g., by a URI or URL) and retrieved from a resource location at a different time. Alternatively, evidence may be stored in a storage region of the computer system (such as a system registry, a configuration file, etc.) or generated dynamically by the computer system or some other source. Thereafter, the code assembly can reference the evidence, which is retrieved from the computer system or other source. A policy manager may also receive evidence that is hard-coded into a membership criterion.

The evidence set 606 is evaluated within the code group collection 608. The arrow 607 represents the input and subsequent processing for the evidence set 606 within the code group collection 608, as described with regard to FIGs. 4 and 5. The code group collection 608 is generated (see arrow 611) by a code group collection generator 610, which receives security policy data read by the parser 612 from the security policy specification 614. The code group collection 608 is in the form of a code group hierarchy in the illustrated embodiment.

In an embodiment of the present invention, each node in the code group hierarchy 608 is associated with a membership criterion, which is represented by the bold line connecting two code group nodes (e.g., membership criterion 618), a child definition (if any), and a code-group permission set (e.g., code-group permission set 616). The root node 620 may also include a membership criterion; however, in one embodiment of the present invention, all code assemblies

are members of the root node. Nevertheless, a more limiting membership criterion may also be associated with the root node.

Evidence from the evidence set 606 is evaluated to determine membership of the code assembly in one or more code groups in the code group hierarchy 608. When a code assembly is determined to be a member of a given code group, the corresponding permission set is associated with the code assembly. In an embodiment of the present invention, the association of a permission set may be dynamically generated. For example, as a result of a determination that the code assembly is a member of a given code group, the code assembly may also be evaluated against the membership criteria of child code groups of the given code group. In addition, an individual permission set of a given code group may be programmatically generated, rather than statically defined. For example, a user may be queried for information to provide enhanced permissions, or available permissions may be different depending on the time of day, or some other variable. A logical set operation may be used to combine or filter the one or more code-group permission sets, as identified by the code-group membership determinations. In one embodiment, a union of all the permission sets of all code groups in which the code assembly is deemed to be a member is used to produce a resulting code-group permission set.

In an exemplary embodiment of the present invention, the policy manager 600 may determine whether an application vendor has licensed appropriate rights to call a library that is installed on the user's computer system. For example, assume that a user has installed an encryption library on a computer system after purchasing a restricted license that allows the user to call the library from a given application. During installation of the library, the security policy is modified to include one or more code groups associated with permissions for calling the library. Each code group is associated with a membership criterion defining conditions for

evaluating evidence associated with the code assembly. Based on these conditions, each element of evidence is treated as either implicitly trusted or initially untrusted.

At some later point, the user may attempt to download and execute a second application that also includes calls to the encryption library. A code assembly within the application may include an embedded certificate, signed by the library vendor, indicating that the code assembly vendor has also purchased rights to call the vendor's library on a user's system. However, because the certificate is provided by the application vendor, the certificate may be untrusted unless it can be independently verified with trusted evidence, such as a key provided by the library vendor. In addition, the key associated with the library may be installed in the computer system, as implicitly trusted evidence, such as by hard-coding the key into the membership criterion or installing it elsewhere within the computer system (or in another trusted location accessible by the computer system). Thereafter, if a given code assembly of the application calls the library, the policy manager 600 evaluates available evidence to determine whether to grant execution permission associated with code assembly's call to the library.

In the library scenario, exemplary initially untrusted evidence 602 may be represented by the certificate issued (signed) by the library vendor in the code assembly indicating that the code assembly is licensed to call the library. Implicitly trusted evidence 604 may be represented by the public key received from library vendor when the library was installed in the computer system. An exemplary membership criterion associated with a library vendor-installed code group, therefore, may have the following form involving two conditions and one logical operation (i.e., an AND operation):

- (1) if the code assembly contains a signed statement indicating a license to call the library vendor's library, [the statement is applied as initially untrusted evidence]

AND

(2) the host verifies that the statement is signed by the library vendor, based on the host-installed public key, [the public key is applied as implicitly trusted evidence]

THEN the code assembly is a member of the library vendor-installed code group and the corresponding permission set is granted to the code assembly to allow the code assembly to call the library.

In an embodiment of the present invention, the operation of applying an element of evidence as either implicitly trusted or initially untrusted involves configuration of logical evidence dependencies (e.g., in a membership criterion) by an installation program, an administration process, a user action, or some other operation. Note that validation of the initially untrusted evidence (e.g. the signed statement) is conditional upon verification by or collaboration with implicitly trusted evidence (e.g., the key). In the above example, the key is designated as implicitly trusted because it does not require further independent verification or self-verification, as specified by the membership criterion of the given code group. However, a membership criterion of another code group may include conditions (1) and (2) and further require an additional condition, which, for example, may test whether the key was installed by an installation program that was executed by an administrator, instead of a normal user. In this second example, the additional condition designates execution of the installation program by an administrator as implicitly trusted evidence, whereas the key itself is initially untrusted.

In the first library example above, there is direct logical dependency between the initially untrusted evidence and the implicitly trusted evidence. A direct logical dependency refers to a membership criterion in which the element of initially untrusted evidence is validated by an individual, although not necessarily unique, element of trusted evidence.

Alternatively, as described in the second library example above, an indirect logical dependency may also be defined in a membership criterion. An indirect logical dependency refers to a membership criterion, for example, in which a first element of initially untrusted evidence must be validated by a second element of initially untrusted evidence that has been validated by a third element of trusted evidence. In addition, one or more elements of initially untrusted evidence may be evaluated in combination with one or more elements of implicitly trusted evidence. An indirect logical dependency allows for evaluation of an evidence chain (or web) in which one or more terminals of the chain are characterized by trusted evidence. In each type of dependency (i.e., direct or indirect), the initially untrusted evidence is eventually validated by implicitly trusted evidence.

To further describe the utility of indirect logical dependencies, one can consider a chain of initially untrusted evidence, which may be referred to as “certificate chain-building” or “certificate path validation”. For example, a code assembly may include signed certificate from library vendor A, stating that the code assembly may access vendor A’s library, which is installed on the user’s system. However, in this scenario, the certificate is signed by potentially trusted vendor B (e.g., VeriSign, which provides Internet trust services). If the host possesses a key with which to verify the signature of vendor B (a direct logical dependency), then the code assembly may be deemed a member of a first code group with an associated permission set that allows execution of the code assembly.

However, if the host does not have a key with which to verify the signature of vendor B, then the code assembly may also include initially untrusted evidence including a statement signed by potentially trusted vendor C (e.g., Microsoft) certifying the certificate signed by vendor B is verified. Accordingly, a second code group may exist that specifies an indirect

dependency in a membership criterion having following form, which includes three conditions and two logical operations (i.e., two AND operations):

- (1) if the code assembly includes (or is associated with) a first signed statement from vendor A and signed by vendor B indicating a license to call vendor A's library, [the first signed statement is applied as initially untrusted evidence]

AND

- (2) the code assembly includes (or is associated with) a second signed statement published and signed by vendor C indicating that the first signed certificate is properly signed by vendor B and can be trusted, [the second signed statement is applied as initially untrusted evidence]

AND

- (3) the host verifies that the second signed statement is signed by vendor C, based on a public key for vendor C installed on the computer system, [the public key is applied as implicitly trusted evidence]

THEN code assembly is a member of the vendor A-installed second code group and the corresponding permission set is granted to the code assembly.

It should be understood that both implicitly trusted evidence and initially untrusted evidence may be, without limitation, stored within the host, hard-coded within a membership criterion, embedded within a code assembly, or retrieved from another resource location or during another network access. In any circumstance; however, the evidence source, evidence version, retrieval timing, user name, etc. may be employed by a membership criterion or evidence resolver to determine the level of trust of a given element of evidence and ultimately the permissions granted to the associated code assembly. It should also be understood that other

conditions and logical operations (e.g., OR, XOR, NOR, NOT, add, subtract, etc.) may be employed within the scope of the present invention.

FIG. 7 illustrates an exemplary system useful for implementing an embodiment of the present invention. An exemplary computing system for embodiments of the invention includes a general purpose computing device in the form of a conventional computer system 700, including a processor unit 702, a system memory 704, and a system bus 706 that couples various system components including the system memory 704 to the processor unit 700. The system bus 706 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus and a local bus using any of a variety of bus architectures. The system memory includes read only memory (ROM) 708 and random access memory (RAM) 710. A basic input/output system 712 (BIOS), which contains basic routines that help transfer information between elements within the computer system 700, is stored in ROM 708.

The computer system 700 further includes a hard disk drive 712 for reading from and writing to a hard disk, a magnetic disk drive 714 for reading from or writing to a removable magnetic disk 716, and an optical disk drive 718 for reading from or writing to a removable optical disk 719 such as a CD ROM, DVD, or other optical media. The hard disk drive 712, magnetic disk drive 714, and optical disk drive 718 are connected to the system bus 706 by a hard disk drive interface 720, a magnetic disk drive interface 722, and an optical drive interface 724, respectively. The drives and their associated computer-readable media provide nonvolatile storage of computer readable instructions, data structures, programs, and other data for the computer system 700.

Although the exemplary environment described herein employs a hard disk, a removable magnetic disk 716, and a removable optical disk 719, other types of computer-readable media

capable of storing data can be used in the exemplary system. Examples of these other types of computer-readable mediums that can be used in the exemplary operating environment include magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, random access memories (RAMs), and read only memories (ROMs).

5 A number of program modules may be stored on the hard disk, magnetic disk 716, optical disk 719, ROM 708 or RAM 710, including an operating system 726, one or more application programs 728, other program modules 730, and program data 732. A user may enter commands and information into the computer system 700 through input devices such as a keyboard 734 and mouse 736 or other pointing device. Examples of other input devices may include a microphone, joystick, game pad, satellite dish, and scanner. These and other input devices are often connected to the processing unit 702 through a serial port interface 740 that is coupled to the system bus 706. Nevertheless, these input devices also may be connected by other interfaces, such as a parallel port, game port, or a universal serial bus (USB). A monitor 742 or other type of display device is also connected to the system bus 706 via an interface, such as a video adapter 744. In addition to the monitor 742, computer systems typically include other peripheral output devices (not shown), such as speakers and printers.

 The computer system 700 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 746. The remote computer 746 may be a computer system, a server, a router, a network PC, a peer device or other
20 common network node, and typically includes many or all of the elements described above relative to the computer system 700. The network connections include a local area network (LAN) 748 and a wide area network (WAN) 750. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the Internet.

When used in a LAN networking environment, the computer system 700 is connected to the local network 748 through a network interface or adapter 752. When used in a WAN networking environment, the computer system 700 typically includes a modem 754 or other means for establishing communications over the wide area network 750, such as the Internet.

5 The modem 754, which may be internal or external, is connected to the system bus 706 via the serial port interface 740. In a networked environment, program modules depicted relative to the computer system 700, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary, and other means of establishing a communication link between the computers may be used.

10 In the illustrated embodiment, a security policy specification may be read from a file on the hard disk drive 712, for example, into memory 704. The CPU 702 executes memory-resident instruction code for a computer processes that implement a virtual machine and that generates a permission grant set for a code assembly received from a resource location based on evidence characterized by different levels of trust. Furthermore, the CPU 702 executes the software components that implement the policy manager recited in the claims.

FIG. 8 illustrates a flow diagram of operations for associating a permission set with a received code assembly based on evidence characterized by different levels of trust in an embodiment of the present invention. Receiving operation 800 receives a first condition and a first evidence element. Receiving operation 802 receives a second condition and a second evidence element. In one embodiment of the present invention, the conditions are received in the form of a membership criterion associated with a code group of a code group collection. The permission set is also associated with the code group. In an alternative embodiment, the conditions may be specified by a security policy specification and applied by an evidence

resolver that evaluates the evidence of the code assembly to determine which evidence may be trusted.

The evidence may be received from a variety of sources, including the code assembly itself, another resource location, and the computer system in which the policy manager is
5 executing. The evidence may also be hard-coded into a condition. Furthermore, evidence is not limited to statically encoded data within the scope of the present invention. For example, the evidence may be generated dynamically by its source before being received in the receiving operations 800 and 802.

Evaluating operation 804 evaluates the first condition using the first evidence element as
10 a parameter. Likewise, evaluating operation 806 evaluates the second condition using the second evidence element as a parameter. Decision operation 810 determines whether both conditions are satisfied. If so, the permission set with which the conditions were associated is then associated with the code assembly in associating operation 808. Decision operation 812
15 determines whether another code group exists against which the code assembly may be evaluated. If so, processing proceeds to the next code group in operation 814 and then repeats the process starting with receiving operation 800. Otherwise, grant operation 816 generates a permission grant set based on the permission set.

In an embodiment of the present invention, the conditions of receiving operations 800
20 and 802 are received in a membership criterion associated with a given code group. The membership criterion is used to determine whether a received code assembly is a member of the given code group. If so, the permission set associated with the code group is associated with the code assembly. In some circumstances, the associated permission set is equivalent to a permission grant set applied against the code assembly during run time. Alternatively, the

permission set, and other permission sets associated with the code assembly, are later processed (e.g., by a permission set generator) using logical set operations. As a result, individual permissions provided in the associated permission set may be omitted, filtered, or merged with other permissions of other associated permission sets.

5 It should be understood, however, that the resulting permission grant set may eventually not include any permissions from an individual permission set associated with code assembly in the associating operation 808. Nevertheless, during processing, individual permission sets from the associating operation 808 are associated with the code assembly based on the conditions and evidence evaluated in evaluating operations 804 and 806, if only to be omitted later. For example, merging and filtering operations performed by permission set generator 518 of FIG. 5 may later omit individual permissions from the resulting permission grant set.

In an alternative embodiment, one or more conditions may be processed to dynamically generate evidence that is thereafter processed by another condition. For example, consider a membership criterion having the following form:

- 10 (1) If the code assembly includes (or is associated with) a first signed statement from vendor A and signed by vendor B indicating a license to call vendor A's library [the first signed statement is designated as initially untrusted evidence], then dynamically generating an indication that this condition (1) is satisfied

AND

- 20 (2) the code assembly includes (or is associated with) a second signed statement published and signed by vendor C indicating that the first signed certificate is properly signed by vendor B and can be trusted [the second signed statement is

designated as initially untrusted evidence], then dynamically generating an indication that this condition (2) is satisfied

AND

(3) the code assembly includes (or is associated with) a third signed statement published and signed by vendor D indicating that the first signed certificate is properly signed by vendor B and can be trusted [the third signed statement is designated as initially untrusted evidence], then dynamically generating an indication that this condition (3) is satisfied

AND

(4) the indications generated by conditions (1), (2), and (3) designate that condition (1) and at least one of conditions (2) and (3) are satisfied [the specified combination of satisfied conditions is designated as implicitly trusted evidence],

THEN the code assembly is a member of the code group associated with the membership criterion and the corresponding permission set is granted to the code.

In this embodiment, the first three conditions generate indications that are received as initially untrusted evidence and processed in condition (4). The result of condition (4) is generated based on the indications received from conditions (1), (2), and (3). Alternatively, condition (4) may also generate one or more additional indication that are received by one or more additional conditions and processed accordingly. Furthermore, weighted or unweighted values may be attributed to conditions that are satisfied and produced as the indications discussed above (e.g., an indication that a condition has been satisfied may be defined by a positive value, whereas an indication that a condition has not been satisfied may be defined by a zero). The values of such conditions may then be evaluated to determine if the code assembly is a member

of the associated code group. For example, if the sum of such values exceeds a predetermined threshold, then the code assembly may be deemed a member of the associated code group.

In another embodiment, negative values may be used to indicate unsatisfied conditions. This embodiment adds another aspect to the evaluation of a code assembly. For example, a condition may have zero value associated with it, if an expected element of evidence is not present in a code assembly (e.g., no certificate is embedded in the code assembly), whereas another condition may have a large negative number if the certificate is found but not properly signed. Thereafter, the results (i.e., the indications) of these conditions may be evaluated alone or in combination with other conditions to determine whether the code assembly is a member of the associated code group. It should be understood that other combinations of conditions and indications may be employed within the scope of the present invention.

The embodiments of the invention described herein are implemented as logical steps in one or more computer systems. The logical operations of the present invention are implemented (1) as a sequence of processor-implemented steps executing in one or more computer systems and (2) as interconnected machine modules within one or more computer systems. The implementation is a matter of choice, dependent on the performance requirements of the computer system implementing the invention. Accordingly, the logical operations making up the embodiments of the invention described herein are referred to variously as operations, steps, objects, or modules.

The above specification, examples and data provide a complete description of the structure and use of exemplary embodiments of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

Claims

WE CLAIM:

1. A method of associating a permission set with a code assembly based on evidence characterized by different levels of trust, the method comprising:

receiving at least a first condition and a first element of evidence, wherein the first condition is associated with the permission set and the level of trust associated with the first element of evidence is independent of other evidence and conditions;

receiving at least a second condition and a second element of evidence, wherein the second condition is associated with the permission set and the level of trust associated with the second element is dependent upon the first condition;

determining whether the first condition is satisfied by the first element of evidence;

determining whether the second condition is satisfied by the second element of evidence;
and

associating the permission set with the code assembly, if both the first condition and the second condition are satisfied.

2. The method of claim 1 wherein the operation of receiving at least a first condition comprises:

receiving the first condition and the first element of evidence within a membership criterion.

3. The method of claim 1 wherein the operation of receiving at least a second condition

comprises:

receiving the second condition and the second element of evidence within a membership criterion.

4. The method of claim 1 wherein the operation of receiving at least a first condition comprises:

receiving the first condition in a membership criterion; and

reading the first element of evidence based on a reference included in the membership

5 criterion.

5. The method of claim 1 wherein the operation of receiving at least a second condition comprises:

receiving the second condition in a membership criterion; and

receiving the second element of evidence based on a reference included in the

5 membership criterion.

6. The method of claim 1 wherein the first condition applies the first element of evidence as implicitly trusted evidence used to validate the second element of evidence applied in the second condition.

7. The method of claim 1 wherein the second condition applies the second element of evidence as initially untrusted evidence.

11. A computer program product encoding a computer program for executing on a computer system a computer process for associating a permission set with a code assembly based on evidence characterized by different levels of trust, the computer process comprising:

generating a collection of code groups, each code group being associated with a

5 membership criterion and a permission set;

receiving the membership criterion associated with one of the code groups, the membership criterion including at least a first condition and a second condition;

referencing a first element of evidence in the first condition, wherein the level of trust associated with the first element of evidence is independent of other evidence and conditions;

10 referencing a second element of evidence in the second condition, wherein the level of trust associated with the second element is dependent upon the first condition;

determining whether the first condition is satisfied by the first element of evidence;

determining whether the second condition is satisfied by the second element of evidence;

evaluating the first condition and the second condition using a logical operation to

15 determine membership of the code assembly in the code group; and

associating the permission set with the code assembly, if the code assembly is determined to be a member of the code group.

12. The computer program product of claim 11 wherein the computer process further comprises:

receiving at least a third condition referencing a third element of evidence, wherein the level of trust associated with the third element is dependent upon the second condition; and

13. A computer data signal embodied in a carrier wave by a computing system and encoding a computer program for executing a computer process associating a permission set with a code assembly based on evidence characterized by different levels of trust, the computer process comprising:

5 receiving at least a first condition referencing a first element of evidence, wherein the first condition is associated with the permission set and the level of trust associated with the first element of evidence is independent of other evidence and conditions;

receiving at least a second condition referencing a second element of evidence, wherein the second condition is associated with the permission set and the level of trust associated with the second element is dependent upon the first condition;

determining whether the first condition is satisfied by the first element of evidence;

determining whether the second condition is satisfied by the second element of evidence;

and

associating the permission set with the code assembly, if both the first and second conditions are satisfied.

14. A computer program storage medium readable by a computer system and encoding a computer program for executing a computer process associating a permission set with a code assembly based on evidence characterized by different levels of trust, the computer process comprising:

5 receiving at least a first condition referencing a first element of evidence, wherein the first condition is associated with the permission set and the level of trust associated with the first element of evidence is independent of other evidence and conditions;

receiving at least a second condition referencing a second element of evidence, wherein the second condition is associated with the permission set and the level of trust associated with the second element is dependent upon the first condition;

determining whether the first condition is satisfied by the first element of evidence;

determining whether the second condition is satisfied by the second element of evidence;

and

associating the permission set with the code assembly, if both the first and second conditions are satisfied.

15. A policy manager for associating a permission set with a code assembly based on evidence characterized by different levels of trust, the policy manager comprising:

a code collection generator generating a collection of code groups, each code group being associated with a membership criterion and a permission set;

5 a membership evaluator evaluating at least a first condition and a second condition associated with one of the code groups, the first condition referencing a first element of evidence in the first condition, wherein the level of trust associated with the first element of evidence is independent of other evidence and conditions; the second condition referencing the second element of evidence, wherein the level of trust associated with the second element is dependent upon the first condition; and

10 a permission set generator associating the permission set of the code group with the code assembly, if the code assembly is determined to be a member of the code group.

16. The policy manager of claim 15 wherein the membership evaluator further receives at least a third condition referencing a third element of evidence, wherein the third condition is associated with the permission set and the level of trust associated with the third element is dependent upon the second condition, and determines whether the third condition is satisfied by

5 the third element of evidence, and

wherein the permission set generator associates the permission set with the code assembly, if the first condition, the second condition, and the third condition are satisfied.

17. A computer program product encoding a computer program for executing on a computer system a computer process for associating a permission set with a code assembly based on evidence characterized by different levels of trust, the computer process comprising:

receiving one or more first conditions, each first condition being associated with one or more first elements of evidence, wherein each first condition is associated with the permission set;

determining whether each first condition is satisfied by an associated first element of evidence;

generating an indication for each first condition that is satisfied;

receiving a second condition associated with the permission set;

determining whether the second condition is satisfied based on the indications; and

associating the permission set with the code assembly, if both the first condition and the second condition are satisfied.

18. The computer program product of claim 17 wherein the indication is associated with a first value associated with the first condition, and the operation of determining whether the second condition is satisfied comprises:

collecting the first value and additional values associated with other satisfied conditions to provide collected values;

summing the collected values to provide a sum; and

evaluating the sum against a threshold to determine whether the second condition is satisfied.

19. The computer program of claim 17 wherein at least one first element of evidence includes initially untrusted evidence.

20. The computer program of claim 17 wherein at least one indication includes initially untrusted evidence.

21. The computer program of claim 17 wherein the computer process further comprises:
generating an indication for each first condition that is not satisfied.

EVALUATING INITIALLY UNTRUSTED EVIDENCE
IN AN EVIDENCE-BASED SECURITY POLICY MANAGER

Abstract of the Invention

An evidence-based policy manager generates a permission grant set for a code assembly received from a resource location. The policy manager executes in a computer system (e.g., a Web client or server) in combination with the verification module and class loader of the run-time environment. The permission grant set generated for a code assembly is applied in the run-time call stack to help the system determine whether a given system operation by the code assembly is authorized. Both code assemblies and evidence may be received from a local origin or from a remote resource location via a network (e.g., the Internet). Evidence having different levels of trust may be evaluated in combination so that a permission grant set is associated only with trusted code assemblies. The policy manager may comprise execution modules for parsing a security policy specification, generating one or more code hierarchies, evaluating membership of the received code assembly in one or more code groups, and generating a permission grant set based upon this membership evaluation.

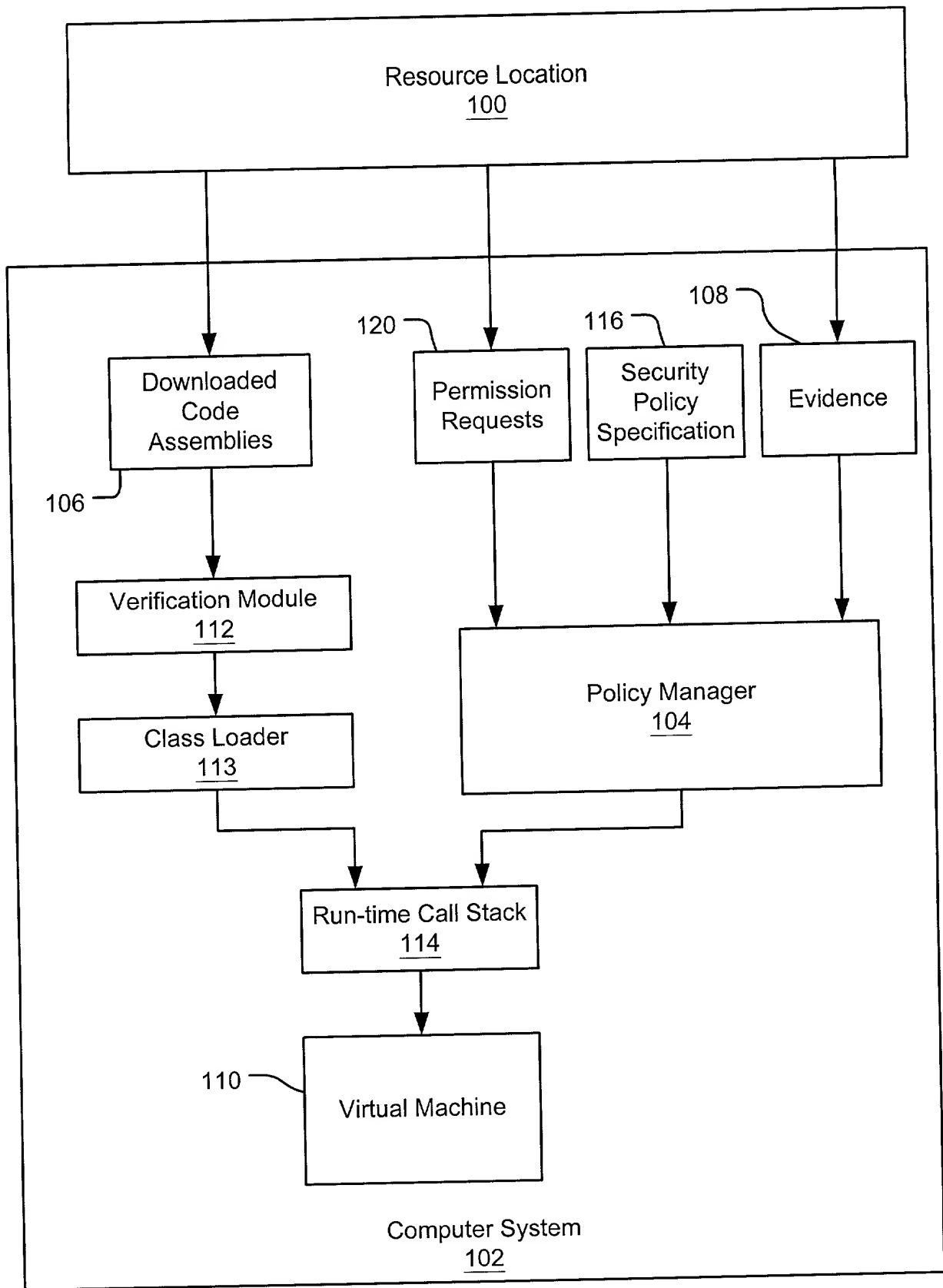


FIG. 1

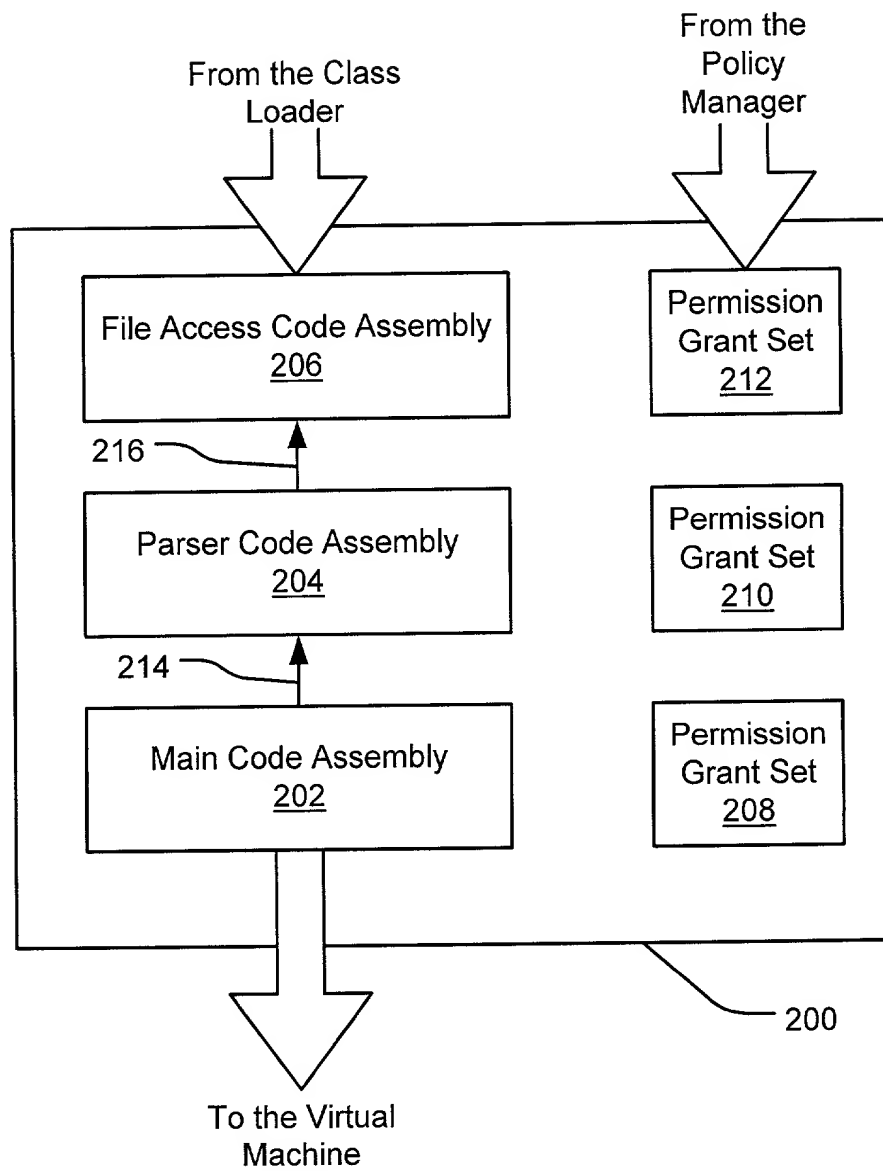


FIG. 2

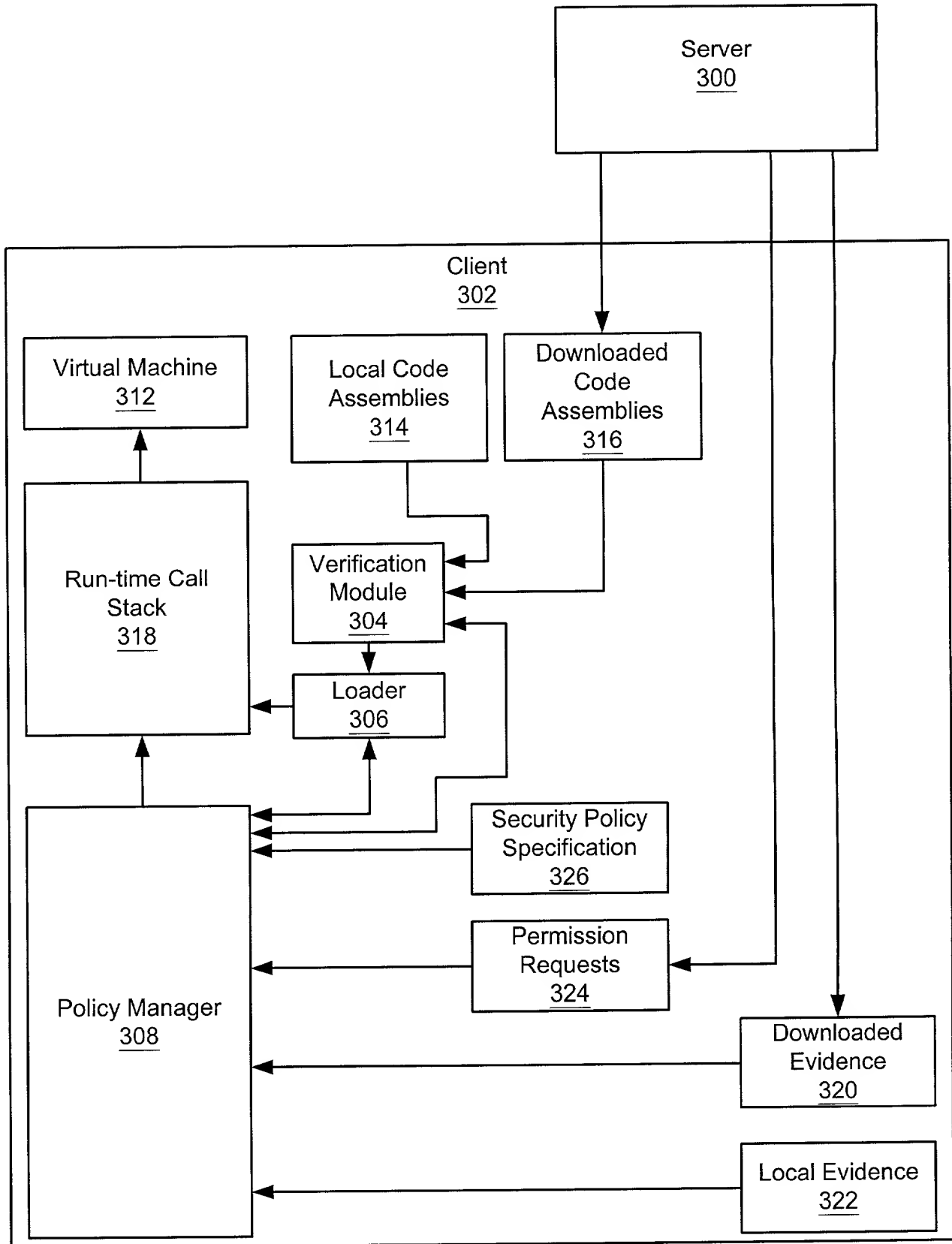


FIG. 3

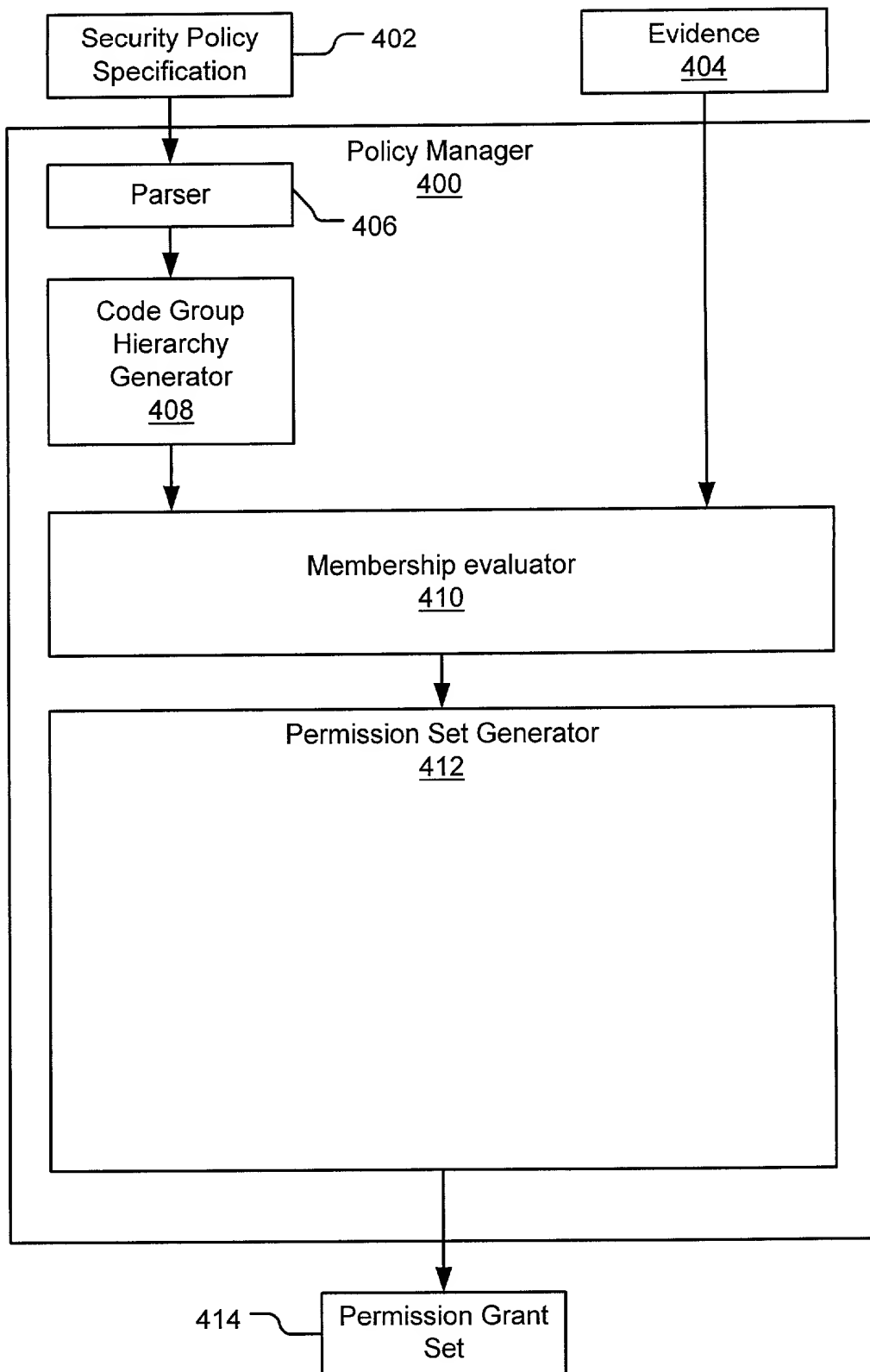


FIG. 4

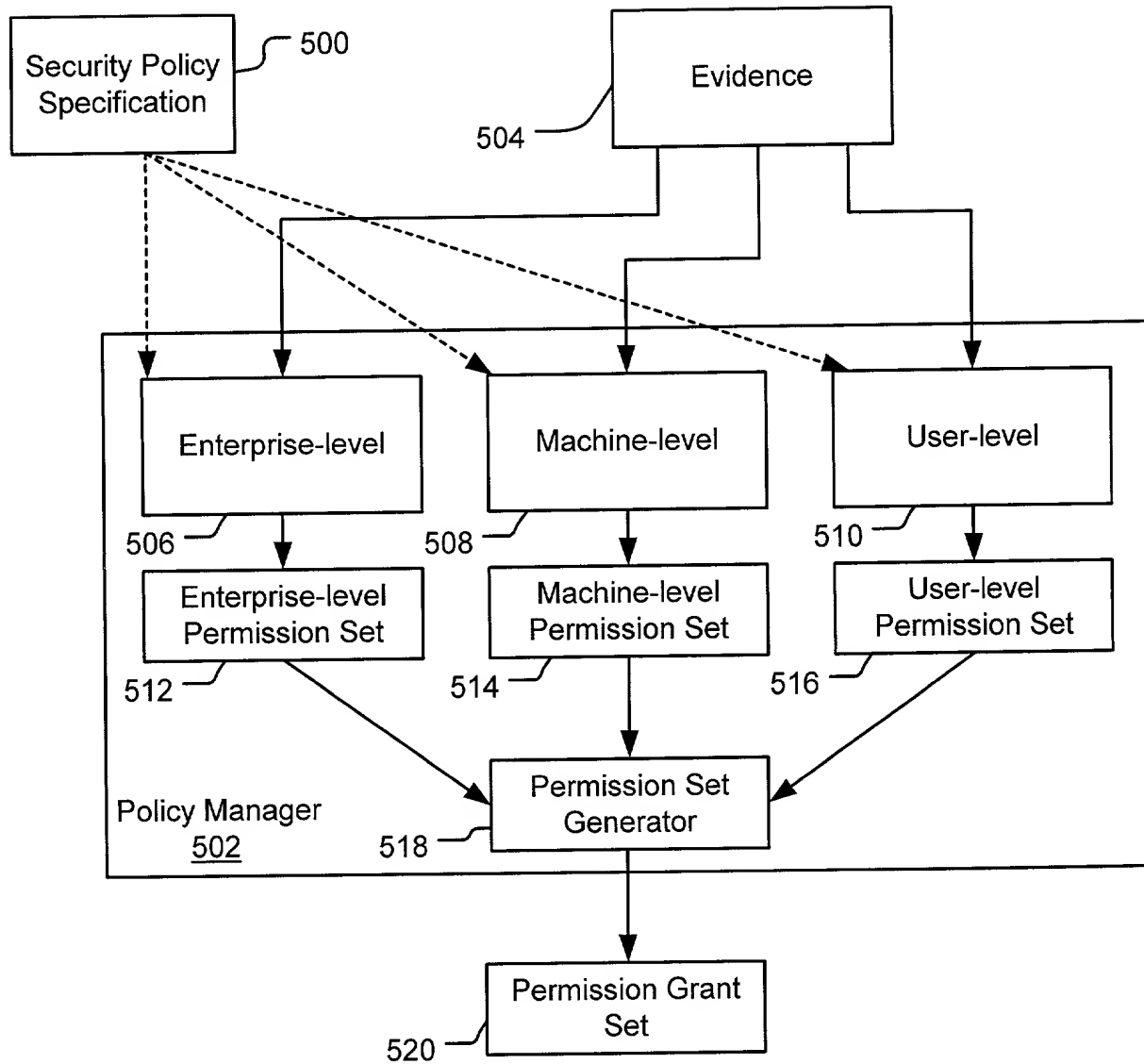


FIG. 5

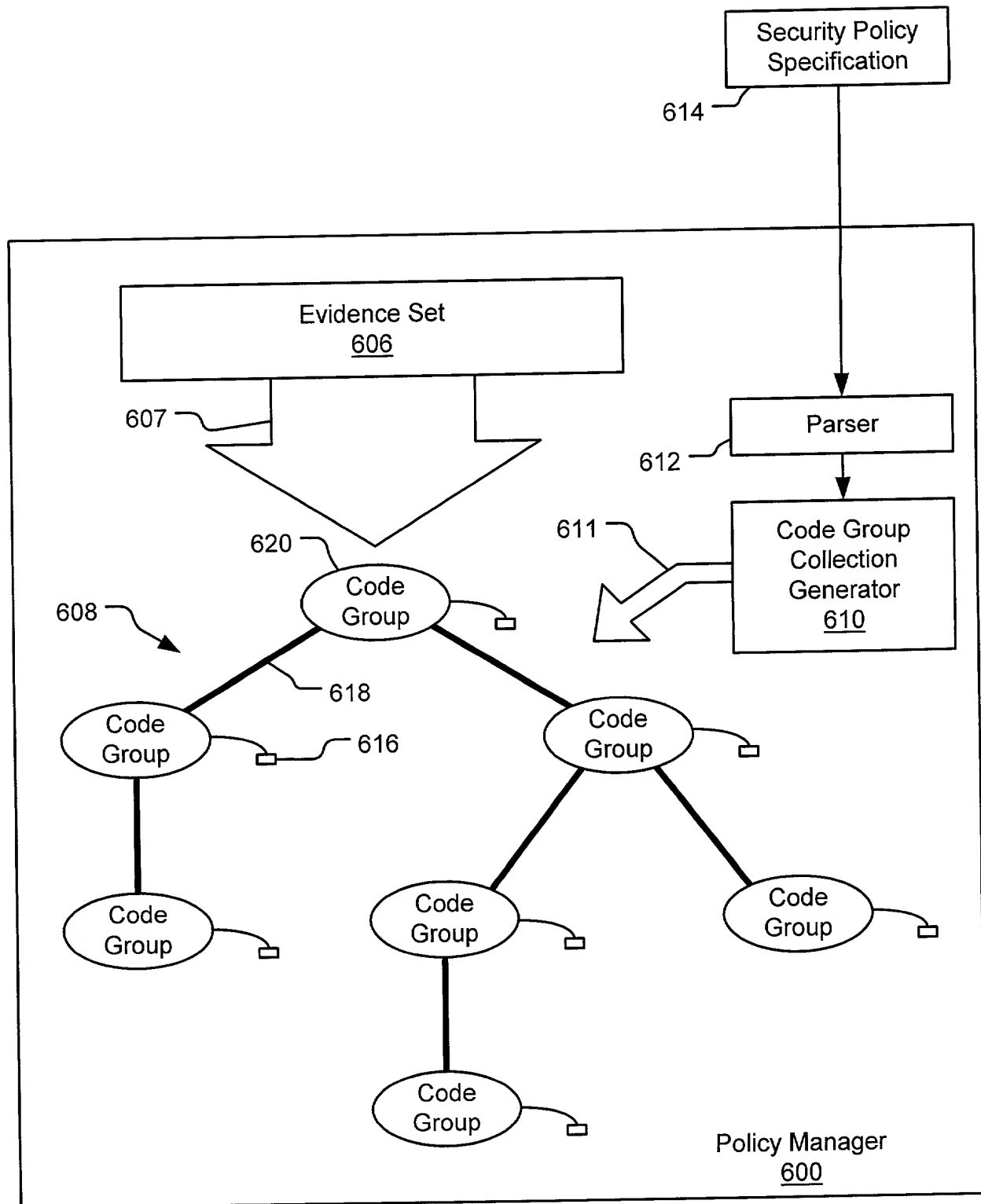


FIG. 6

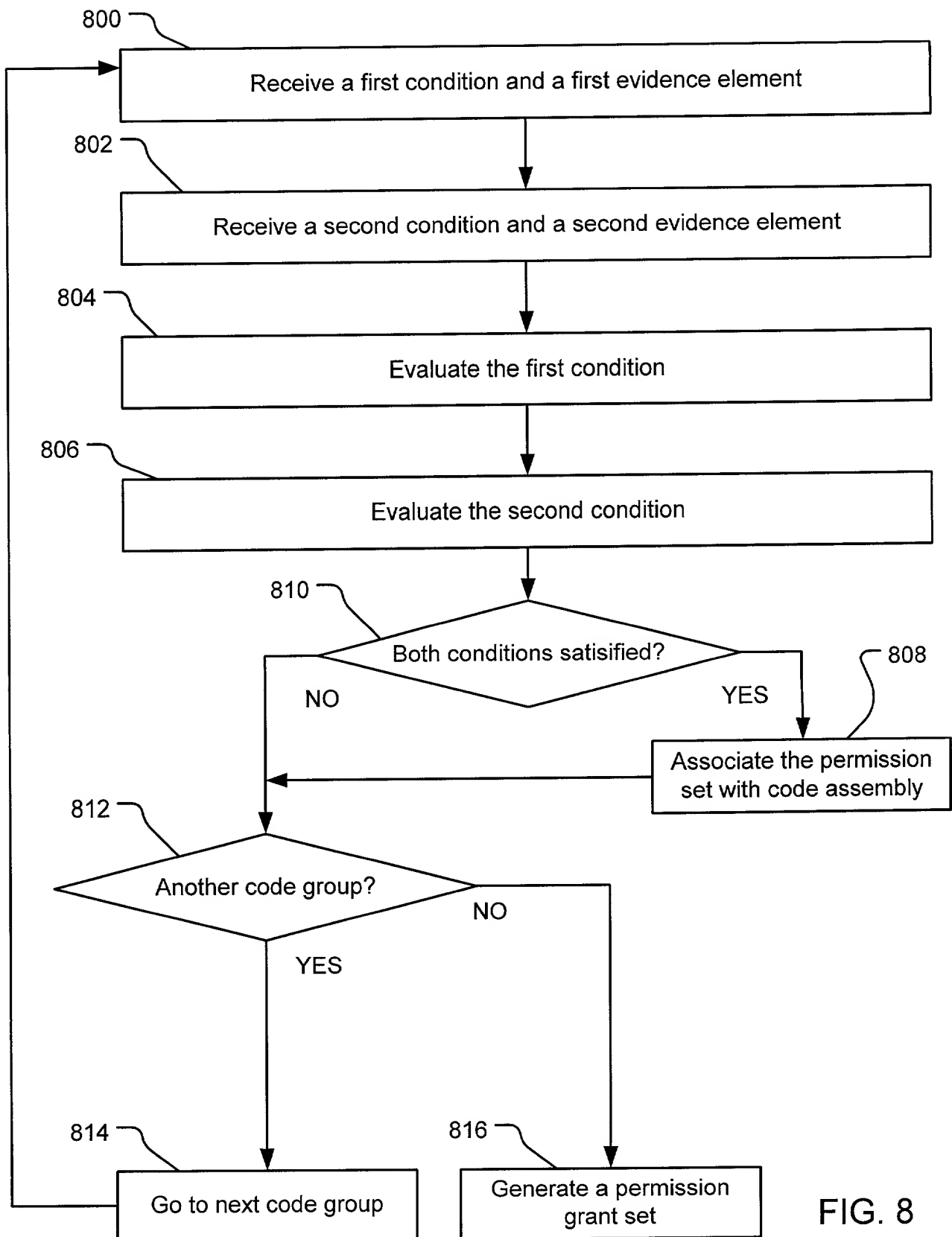


FIG. 8

MERCHANT & GOULD P.C.

United States Patent Application

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor I hereby declare that my residence, post office address and citizenship are as stated below next to my name; that

I verily believe I am the original, first and a joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled EVALUATING INITIALLY UNTRUSTED EVIDENCE IN AN EVIDENCE-BASED SECURITY POLICY MANAGER, the specification of which is attached hereto, which I have reviewed and for which I solicit a United States patent.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56 (attached hereto).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119/365 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on the basis of which priority is claimed:

- a. ☒ no such applications have been filed.
 b. ☐ such applications have been filed as follows:

FOREIGN APPLICATION(S), IF ANY, CLAIMING PRIORITY UNDER 35 USC § 119			
COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)

ALL FOREIGN APPLICATION(S), IF ANY, FILED BEFORE THE PRIORITY APPLICATION(S)			
COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)

I hereby claim the benefit under Title 35, United States Code, § 120/365 of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. APPLICATION NUMBER	DATE OF FILING (day, month, year)	STATUS (patented, pending, abandoned)

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below:

U.S. PROVISIONAL APPLICATION NUMBER	DATE OF FILING (Day, Month, Year)

I hereby appoint the following attorney(s) and/or patent agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith:

Albrecht, John W.	Reg. No. 40,481	Lacy, Paul E.	Reg. No. 38,946
Anderson, Gregg I.	Reg. No. 28,828	Larson, James A.	Reg. No. 40,443
Ansems, Gregory M.	Reg. No. 42,264	Liepa, Mara E.	Reg. No. 40,066
Batzli, Brian H.	Reg. No. 32,960	Lindquist, Timothy A.	Reg. No. 40,701
Beard, John L.	Reg. No. 27,612	Lycke, Lawrence E.	Reg. No. 38,540
Berns, John M.	Reg. No. 43,496	McAuley, Steven A.	Reg. No. P-46,084
Black, Bruce E.	Reg. No. 41,622	McDonald, Daniel W.	Reg. No. 32,044
Branch, John W.	Reg. No. 41,633	McIntyre, Jr., William F.	Reg. No. P-44,921
Bremer, Dennis C.	Reg. No. 40,528	Mueller, Douglas P.	Reg. No. 30,300
Bruess, Steven C.	Reg. No. 34,130	Pauly, Daniel M.	Reg. No. 40,123
Byrne, Linda M.	Reg. No. 32,404	Phillips, John B.	Reg. No. 37,206
Carlson, Alan G.	Reg. No. 25,959	Phunkett, Theodore	Reg. No. 37,209
Caspers, Philip P.	Reg. No. 33,227	Prendergast, Paul J.	Reg. No. 46,068
Chiapetta, James R.	Reg. No. 39,634	Pytel, Melissa J.	Reg. No. 41,512
Clifford, John A.	Reg. No. 30,247	Qualey, Terry	Reg. No. 25,148
Cochran, William W.	Reg. No. 26,652	Reich, John C.	Reg. No. 37,703
Daignault, Ronald A.	Reg. No. 25,968	Reiland, Earl D.	Reg. No. 25,767
Daley, Dennis R.	Reg. No. 34,994	Schmaltz, David G.	Reg. No. 39,828
Dalglish, Leslie E.	Reg. No. 40,579	Schuman, Mark D.	Reg. No. 31,197
Daulton, Julie R.	Reg. No. 36,414	Schumann, Michael D.	Reg. No. 30,422
Devries Smith, Katherine M.	Reg. No. 42,157	Scull, Timothy B.	Reg. No. 42,137
DiPietro, Mark J.	Reg. No. 28,707	Sebald, Gregory A.	Reg. No. 33,280
Edell, Robert T.	Reg. No. 20,187	Skoog, Mark T.	Reg. No. 40,178
Epp Ryan, Sandra	Reg. No. 39,667	Spellman, Steven J.	Reg. No. 45,124
Glance, Robert J.	Reg. No. 40,620	Stoll-DeBell, Kirstin L.	Reg. No. 43,164
Goggin, Matthew J.	Reg. No. 44,125	Storer, Shelley D.	Reg. No. P45,135
Golla, Charles E.	Reg. No. 26,896	Sumner, John P.	Reg. No. 29,114
Gorman, Alan G.	Reg. No. 38,472	Summers, John S.	Reg. No. 24,216
Gould, John D.	Reg. No. 18,223	Swenson, Erik G.	Reg. No. 45,147
Gregson, Richard	Reg. No. 41,804	Tellekson, David K.	Reg. No. 32,314
Gresens, John J.	Reg. No. 33,112	Trembath, Jon R.	Reg. No. 38,344
Hamre, Curtis B.	Reg. No. 29,165	Underhill, Albert L.	Reg. No. 27,403
Hillson, Randall A.	Reg. No. 31,838	Vandenburgh, J. Derek	Reg. No. 32,179
Holzer, Jr., Richard J.	Reg. No. 42,668	Wahl, John R.	Reg. No. 33,044
Johnston, Scott W.	Reg. No. 39,721	Weaver, Karrie G.	Reg. No. 43,245
Kadievitch, Natalie D.	Reg. No. 34,196	Welter, Paul A.	Reg. No. 20,890
Karjeker, Shaukat	Reg. No. 34,049	Whipps, Brian	Reg. No. 43,261
Kastelic, Joseph M.	Reg. No. 37,160	Wickhem, J. Scot	Reg. No. 41,376
Kettelberger, Denise	Reg. No. 33,924	Williams, Douglas J.	Reg. No. 27,054
Keys, Jeramie J.	Reg. No. 42,724	Witt, Jonelle	Reg. No. 41,980
Knearl, Homer L.	Reg. No. 21,197	Wu, Tong	Reg. No. 43,361
Kowalchyk, Alan W.	Reg. No. 31,535	Xu, Min S.	Reg. No. 39,536
Kowalchyk, Katherine M.	Reg. No. 36,848	Zeuli, Anthony R.	Reg. No. P45,255

In addition, I also hereby appoint the following attorneys to prosecute this application and to transact all business in the U.S. Patent and Trademark Office in connection therewith:

Kate E. Sako, Reg. No. 32,628
Daniel D. Crouse, Reg. No. 32,022

I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/ organization who/which first sends/sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Merchant & Gould P.C. to the contrary.

Please direct all correspondence in this case to Merchant & Gould P.C. at the address indicated below:

Homer L. Knearl
 Merchant & Gould P.C.
 P.O. Box 2903
 Minneapolis, MN 55402-0903
 303.357.1633

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2 0 1	Full Name Of Inventor	Family Name LaMacchia	First Given Name Brian	Second Given Name A.
	Residence & Citizenship	City Seattle	State or Foreign Country Washington	Country of Citizenship United States of America
	Post Office Address	Post Office Address 524 12 th Avenue East, # 201	City Seattle	State & Zip Code/Country Washington 98102/USA
Signature of Inventor 201:				Date:
2 0 3	Full Name Of Inventor	Family Name Kohnfelder	First Given Name Loren	Second Given Name M.
	Residence & Citizenship	City Bellevue	State or Foreign Country Washington	Country of Citizenship United States of America
	Post Office Address	Post Office Address 14121 NE 2 nd Street	City Bellevue	State & Zip Code/Country Washington 98007-6937/USA
Signature of Inventor 202:				Date:
2 0 3	Full Name Of Inventor	Family Name Fee	First Given Name Gregory	Second Given Name Darrell
	Residence & Citizenship	City Kirkland	State or Foreign Country Washington	Country of Citizenship United States of America
	Post Office Address	Post Office Address 12036 100 th Avenue NE, Apt. # E303	City Kirkland	State & Zip Code/Country Washington 98034/USA
Signature of Inventor 203:				Date:

§ 1.56 Duty to disclose information material to patentability.

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is canceled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is canceled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§ 1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim;

or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application:

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.